10TH INTERNATIONAL COMMAND AND CONTROL RESEARCH AND TECHNOLOGY SYMPOSIUM
THE FUTURE OF C2

Intent Driven Adversarial Modeling

MODELING AND SIMULATION

Authors

Duane A. Gilmour
Air Force Research Laboratory/IFTC
26 Electronic Parkway
Rome, NY 13441-4514
Duane.Gilmour@rl.af.mil
315.330.3550

Lee S. Krause
Securboration
695 Sanderling Drive
Indialantic, FL 32903
lkrause@securboration.com
321.591.9836

Lynn A. Lehman,
Securboration,
695 Sanderling Drive
Indialantic, FL 32903
llehman@securboration.com
919.367.0087

Dr. Eugene Santos, Jr
Intelligent Distributed Information Systems Laboratory
University of Connecticut
eugene@cse.uconn.edu
860.486.5955

Dr. Qunhua Zhao
Intelligent Distributed Information Systems Laboratory
University of Connecticut
qzhao@cse.uconn.edu
860.486.4492

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2005		**00-00-2005 to 00-00-2005**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Intent Driven Adversarial Modeling	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Air Force Research Laboratory,AFRL/IFTC,26 Electronic Parkway,Rome,NY,13441-4514**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**43**	

Abstract

Modern elements of military intelligence and decision making require predictions of adversary force actions and reactions to provide a complete and realistic viewpoint. Current methods for providing realistic adversary force simulation are largely manual processes. Adversarial simulation requires continual assessment of friendly courses of action and is currently "human assessment capability" limited. To develop a computational model of dynamic adversary behaviors that includes the ability to integrate with intelligence and mission data sources, computational models must address operational patterns, behaviors, or doctrines of present-day adversaries (terrorist cells, local insurgents, guerillas, and armed thugs) as well as more conventional force elements. The dynamic nature of adversary force behavior with respect to the changing capabilities, biases, beliefs, goals, intentions, and perceptions of friendly force actions must be addressed. The Emergent Adversarial Modeling System (EAMS) addresses these elements through explicit focus on adversarial intent as a driver for adversarial response. Specific capabilities address the changing nature of adversary composition. This paper will discuss the results of the ongoing EAMS research project into adversarial modeling and adversarial response simulation.

Key Words:

Bayesian Net, Bayesian Knowledge Base, Adversarial Modeling, Emergent Behavior, Adversary Intent

Introduction

The increase in limited conflict warfare has created new challenges in mission planning and simulation. New approaches to warfare planning, such as effects based operations and predictive battlespace awareness, have also increased the need for improved simulations. An important part of simulation for mission planning is the creation and exercise of realistic adversary responses to friendly force actions. Typical "flipped" response approaches, while adequate when facing a doctrine based opponent are no longer sufficient with the types of less predictable, less organized adversary forces commonly faced in modern battlefield scenarios. The Emergent Adversarial Modeling System, or EAMS, is under development to address this shortfall. EAMS is being developed by a team of researchers from Securboration and the University of Connecticut under the direction of the Information Directorate of the Air Force Research Laboratory.

The objective of EAMS is to provide a realistic simulation that supports and incorporates emergent behavior of Red (adversary) force in response to Blue (friendly) force actions. In cold war era conflicts where likely adversaries were expected to exhibit similar capabilities and doctrine to Blue forces, attrition based simulations achieved capable results. In the post-cold war era of limited conflict and unconventional adversary response, simulations based on attrition principles do not yield realistic or useable results. Today's non-conventional adversaries seldom have capabilities that rival U.S. or coalition forces in technology or technique. In these cases, adversarial intent and response behavior become far more important considerations. EAMS demonstrates alterations of Red force behavior in response to observed Blue force actions. Those Blue force actions are addressed from the perspective of the Red force (i.e. what does Red think or believe that Blue is doing (Santos 2003)). EAMS shows how modifications in Blue force behavior and actions directly affect or modify Red force responses. This type of fluid, dynamic response moves beyond the attrition based "who can knock out what first" doctrine and provides military planners and intelligence analysts with a more realistic simulation of adversarial actions. The realistic modeling of emergent adversarial behavior is important in the evolution of new methodologies, like Predictive Battlespace Awareness. EAMS works in concert with other Securboration and Air Force tools to provide a rich simulation environment.

To provide a complete and realistic viewpoint, modern elements of military intelligence and decision making require predictions of adversary force actions as well as reactions of that adversary force to friendly actions. This realistic point of view is represented by methods associated with Intelligence Preparation of the Battlespace (IPB). In current systems and approaches, producing such predictions and properly accounting for them, is largely a manual process. The necessary assessment and continual re-assessment of friendly courses of action is currently limited by the human assessment capability at hand. EAMS is a computational model of dynamic adversary behaviors that includes the ability to integrate with various intelligence and mission data sources (Modernized Integrated Database (MIDB), Air Operations Database (AODB), IPB Products, etc.). EAMS addresses operational patterns, behaviors, and doctrines of present-day adversaries (terrorist cells, local insurgents, guerillas, and armed thugs) as well as more conventional force elements. Further complications of simulating adversarial actions

arise from the complexity of the battlefield, the uncertainty inherent from fog-of-war, and active adversary deceptions and ruses. To provide a meaningful simulation environment, the dynamic nature of Red force behavior with respect to EAMS addresses the changing capabilities, biases, beliefs, goals, intentions, and perceptions of Blue force actions. Specific capabilities address the changing nature of adversary composition through expansion of adversary parameterization concepts. Adversary parameterization allows the construction or "build-up" of adversaries from a library of capabilities, goals, intentions, etc. (Santos and Negri 2004).

Realistic adversarial behavior must be dynamic and fluid as Red force elements learn and adapt to Blue force actions, both current and prior. These adversary behaviors must also take into account potential Red force elements that engage in operations with indirect intentions (e.g. sway public or world opinion, inject fear into a local population, curry favor with journalists, etc.). Elements of adversarial intent become mainline predictors of actions as, especially in limited warfare scenarios; objectives of an adversary force become more long-term in nature and may be driven by non-conventional objectives or tactical goals. The objective of EAMS is to provide a realistic simulation that supports emergent behavior of Red force actions/reactions based on Blue force actions. EAMS addresses these elements through explicit focus on adversarial intent as the primary driver of adversarial response.

Background

The military planning process depends upon analysis systems to anticipate and respond in real-time to a dynamically changing battlespace with counteractions. Complex technical challenges exist in developing automated processes to derive hypotheses about future alternatives for mission scenarios. The military conducts combat operations in the presence of uncertainty and the alternatives that might emerge. It is virtually impossible to identify or predict the specific details of what might transpire. Plans and strategies, which result in courses of action (COAs), are evaluated to determine the necessary steps to meet the overall strategic objectives. COA analysis, also defined as wargaming, is the process of performing "what if" analysis of actions and reactions designed to visualize the flow of the battle and evaluate each friendly COA. Currently, COAs are evaluated by two techniques. One technique involves teams of individuals playing out both sides of a campaign, while trying to predict the outcome based on each others actions. This technique is manpower intensive, and cannot be maintained at the speed of current operations. The second technique involves automated wargaming technologies. Automated techniques are faster than manual approaches; however, they are performed against a scripted adversary and focus on attrition based modeling, neither of which is representative of current campaigns. Because current generation wargaming technologies execute a pre-scripted sequence of events for an adversary, or Red force, independent of the Blue force actions, the results typically do not last beyond the first campaign action.

A significant research challenge for wargaming is predicting and assessing how Blue force actions result in adversary behavioral outcomes, and how those behavioral outcomes impact the adversary commander's decisions and future actions. Conventional wargames are also insufficient when it comes to evaluating modern campaign

approaches. They focus on traditional attrition based force-on-force modeling, whereas modern campaign strategies employ and evaluate a mixture of kinetic and non-kinetic operations. The military is pursuing effects based operations (EBO) as one such campaign approach (Fayette 2001). EBO is an approach to planning, executing and assessing military operations that focuses on obtaining a desired strategic outcome or "effect" on the adversary instead of merely attacking targets or simply dealing with objectives. For wargames to be effective, they must allow users to evaluate multiple ways to accomplish the same goal with a combination of direct, indirect, complex, cumulative, and cascading effects. The focus of this research is to develop techniques to model adversarial behaviors that will provide a simulation capability that intelligently anticipates potential adversarial actions for dynamic adversary COA analysis. Such a system will allow planners to better evaluate the effectiveness of today's alternative decisions and plans in tomorrow's battlefield.

The Case for Adversarial Modeling

In the current world environment, the rapidly changing dynamics of adversarial operations are increasing the difficulty for military analysts and planners to accurately predict potential adversarial actions. As an integral part of the planning process, analysts need to be able to assess planning strategies against the range of potential adversarial actions. When the first decision in a given COA is implemented, subsequent decisions must be evaluated based on the new state of the world. This sequential action/reaction analysis concept requires predictive adversary models and these models are vital in assessing planned military decisions. For wargaming tools to be of greater use to military analysts and planners, they must incorporate models of adversarial behaviors that accurately predict potential adversarial actions. Traditionally, friendly COAs are wargamed against the "most likely" and "most dangerous" adversary COAs, both of which are a pre-scripted sequence of events, independent of the Blue force actions.

Techniques are being investigated into the feasibility of utilizing an adversarial tool as a core element within a predictive simulation to establish emergent adversarial behavior (Santos 2003, Surman et al. 2003, Santos and Negri 2004). Emergent behavior refers to intelligent dynamic adversarial actions generated at the operational level in response to the execution of the friendly force within the simulation. Multiple adversarial models with varying belief systems would be capable of automatically posing different actions and counteractions (Surman et al. 2003). The desire is to use intelligent adversary models to generate alternative futures in performing COA analysis. A significant amount of uncertainty accompanies any adversarial modeling capability. This uncertainty encompasses the process of decision making in a dynamic situation. Typically, models are abstractly created to reflect the adversary's beliefs, goals, and intentions; all of which are based on friendly interpretation of the adversary. The uncertainty of this adversarial decision process makes it necessary to evaluate friendly COAs against a range of adversary COAs. Also, based on analysts' interpretations of the adversary, numerous reactions are possible in response to a friendly action. The capturing of these action/reaction dynamics is essential to the future of the COA analysis process. By simulating numerous COAs prior to and during engagement, it may be possible to estimate outcomes of adversary actions immediately after they are accomplished within

an operational situation. This will allow decision makers to better respond to a dynamic and volatile adversary during execution, with counter actions.

Changes to Support the New Planning Paradigm

Existing (or potential) approaches for predicting adversary actions, such as game theoretic and game playing, adversarial planning, and pattern recognition (will) at best provide partial/limited solutions and do not satisfy the intent or expectations. In today's gaming industry, the majority of the gaming software is finite state machine (FSM) based. The FSMs employ conditions to determine if a transition should occur and ad-hoc ordering to determine which one to pick first. In this case, numerous behaviors are constructed and composed in some manner. With this approach, the classic problem of building enough behaviors is potentially even more constrained and lacks a theoretical basis. Also, pre-defined behaviors can not represent a dynamic notion of uncertainty in the adversary behavior.

Chess style approaches rely on the assumption that the values of the pieces are static; values of objectives are static, etc. However, in reality, there are massive dynamics involved in any real combat situations. For reactive and deliberative planning approaches to adversarial modeling, they are easily stymied by temporal and uncertainty issues, as well as succumbing to scalability. In the case of pattern recognition approaches, the largest difficulty encountered is the opaqueness of the results to the user. While patterns of adversarial behavior can be effectively identified, the explanation of these behaviors and how they are related to (or derived from) the observable is fundamentally lacking. Thus, proper mechanisms for assisting the user in analyzing the situation (what-if, deception analyses, etc.) are not available.

Predictive adversary modeling is one of the key requirements for EBO, where the adversary is addressed as a system. An EBO approach is actually an intent driven approach, where the purpose, the desired end state, method and risk of a military mission are considered. Thus, one of the greatest technological challenges for the EBO approach is to model adversarial decision making. Another major defect of the approaches discussed previously is that they fail to consider the necessity of understanding, modeling, and inferring adversary intentions. They focus almost exclusively on adversarial capabilities and doctrines. It is very difficult to incorporate "soft factors" (as described below) into these approaches. As a result, the adversary themselves, who actually make the decisions and respond in a dynamic environment, are largely ignored. It is clearly impossible for these approaches to properly assess the goals, beliefs, or desired end-states of the adversary.

Soft factors are those factors that influence adversarial intent in their decision making process, which include social, cultural, religious, political, economic and psychological issues. Soft factors are complex and hard to quantify; many of them are human oriented. Although military strategists have long advocated the need to understand the adversary, the existing approaches are mainly capability focused. It is even said that we can judge the adversaries capabilities but not their intentions (Grabo 2002), since it is difficult to judge the intentions that are highly influenced by soft factors. However, it must be

realized that to accurately assess the adversary's capabilities is also difficult, even when the information is readily obtainable; where, in reality, dealing with uncertain, incomplete, and even deceptive information is almost unavoidable (Grabo 2002). Soft factors are key elements that must be accounted for in the EBO approach, starting from the commander's intent, such as their desired end states. Even a single soft factor, for example, a personality factor of an individual, can change the possible actions taken by the individual which ultimately affect the range of available options for their opponents.

Human decision making is greatly influenced by the context of personal experience, the personality that has been formed within the unique experience, and other soft factors. The states of the soft factors in this context decide an individual's (or a group of individuals') understanding of what happened and is happening and their judgment of what will happen, what can be done, and what should be done. By influencing what the adversary believes about themselves and their beliefs about the friendly force, soft factors eventually influence their goals (desired effects), which decide what kind of COAs they are going to pursue. Furthermore, derivation of a single soft factor, such as "aggressiveness", often involves the derivation and combination of influences from several supporting soft factors.

Emergent Adversarial Modeling

General Karl von Clausewitz said that the major difference between real war and war on paper is that real war is fought against an intelligent being that reacts. Traditionally, predictions of adversary behavior are by in large provided through a manual process, and are predefined. In reality, adversarial behavior emerges during the interactions/encounters between Red force and Blue force. The adversary force reacts, and also learns from and adapts to Blue force actions. There is a significant amount of uncertainty associated with any emergent adversarial actions.

EAMS is created to describe and predict adversary's beliefs, goals, and potential actions. The uncertainty of the adversarial decision making process makes it necessary to evaluate a range of adversarial COAs in response to Blue actions. EAMS provides opportunities of conducting "what-if" analysis for the Blue user, which enables analysts to investigate the alternative emergent behavior in different situations, and make well-informed decisions.

Since the adversarial behavior and COAs are obviously influenced in a cause-and-effect manner, the ability to trace the adversarial intent, such as what are the desired end states and why, is the key for a realistic adversary model. Especially in today's asymmetric environment, the adversary almost always tries to seek out non-conventional actions that do not follow the traditional force-on-force doctrines, to surprise the friendly forces. In EAMS, the prediction of the adversarial behavior in response to Blue actions is based upon their intent. The model is also capable of evolving, according to the changes of capabilities, biases, beliefs, goals, intentions, and perceptions of Blue force actions. Therefore, EAMS can provide a realistic simulation of the adversary.

EAMS: An Intent Driven Approach of Predicting Emergent Adversarial Behavior

Increasingly, in modern warfare scenarios, adversaries are driven by intent rather than doctrine. Due to many factors, non-conventional forces cannot survive long term in an attrition based conflict. This reality moves adversary intent to the forefront in terms of a driver of adversary action and response. Responses often fall outside of limited warfare response actions and address larger or more far reaching political, economic and social goals. In many limited warfare scenarios, it becomes of paramount importance to address non-conventional adversary response driven by intent rather than tactical objectives. EAMS addresses the importance of intent-driven adversarial behavior. EAMS specifically focuses on intent as the catalyst to produce realistic adversary response. In intent driven warfare, specific beliefs, observations and perceptions drive non-conventional responses.

Red goals and intentions occur at numerous levels, from high level strategic goals through operational and tactical goals. As long-term and short-term goals of an adversary change, EAMS components capture changes according to a three-component architecture comprising an: Adversary Rationale Network (why), Adversary Action Network (how), and Adversary Goals (what.) The rationale network is a Bayesian knowledge base consisting of adversary axioms (beliefs about themselves such as "divine mandate"), adversary beliefs (what they believe or have observed concerning Blue forces), adversary goals (strategic plans), and highest-level adversary actions (e.g., preserve launchers) (Santos 2003). *Note that in EAMS adversary actions are considered highest-level if they are not the sub-goal (traditional planning) of some other action.* EAMS takes inputs from multiple sources:

1. Evidence/observables from battlefield, recon, sensor arrays, etc.
2. Projected Red COAs from the adversarial specification represented by an instance in the EAMS Ontology.
3. Analyst inputs from the Intelligence Situation Processor (ISP) component of EAMS, critical to merging and working with human analysts.

A complete system must encompass all three inputs to complete the cycle of Red force analyses and to be incorporated into Blue force planning. The EAMS Ontology and the ISP will be discussed in more detail in the next section.

The basic adversary intent architecture consists of three core components:

1. **Goals/Foci**: A prioritized (by probability) list of short and long term goals representing adversary intents, objectives or foci. The goal component captures ***what*** the adversary is doing.
2. **Rationale Network**: A probabilistic network representing the influences of the adversary's beliefs, both about themselves and their opposition, on their goals and on high level actions associated with those goals. The rationale component infers ***why*** the adversary is behaving in a certain fashion.

3. **Actions Network**: A probabilistic network representing the detailed relationships between adversary goals and possible actions to realize those goals. The action component captures ***how*** an adversary might act.

Due to the inherent uncertainty involved in adversary course of action prediction, Bayesian knowledge bases (BKBs) will be used as the primary knowledge representation for the rationale and action networks. Each random variable (RV) involved in the BKBs is classified into one of four classes: *axioms, beliefs, goals,* and *actions*.

1. **Adversary axioms (X)** – represent the underlying beliefs of the adversary about themselves (vs. beliefs about Blue forces). Axioms typically serve as inputs or explanations to the other RVs, such as adversary goals.
2. **Adversary beliefs (B)** – represent the adversary's beliefs regarding Blue forces (e.g., an adversary may believe that U.S. forces will not destroy religious sites or shrines).
3. **Adversary goals (G)** – represent the goals or desired end-states of the adversary (e.g., preserving launchers, damage world opinion of U.S. action, defeat U.S. foreign policy, etc.).
4. **Adversary actions (A)** – represent the actions of the adversary that can typically be observed by Blue forces.

This structure permits explicit representation of adversarial intent so that intent can be utilized as a primary driver of adversarial response. The construction of the probabilistic networks for reasoning is a process of identifying potential adversarial goals based on what the adversary believes about the friendly force and themselves. Possible actions are then generated that can be carried out to achieve these goals based on their capabilities and recent actions. Both the adversary capabilities and potential actions are evaluated in the light of their intentions, where soft factors can be reflected by the axiom and/or belief variables in the model. This approach naturally creates the desired "push-pull" effect in Blue vs. Red force interactions. This capability affords military planners and analysts a more realistic capability in the evaluation of alternative Blue force COAs without the extensive level of manual interaction currently required.

The EAMS Proof of Concept

As part of the initial EAMS effort, a prototype "proof of concept" (POC) demonstration was constructed. The intent of the POC was to demonstrate the feasibility of approaches employed by EAMS and validate dynamic adversary response behavior. The POC made use of existing systems, capabilities and technologies to enhance the capability and to demonstrate EAMS interoperability with existing systems. EAMS exploitation of existing development efforts facilitated a meaningful and robust demonstration. A summary level view of the demonstration is shown in Figure 1.

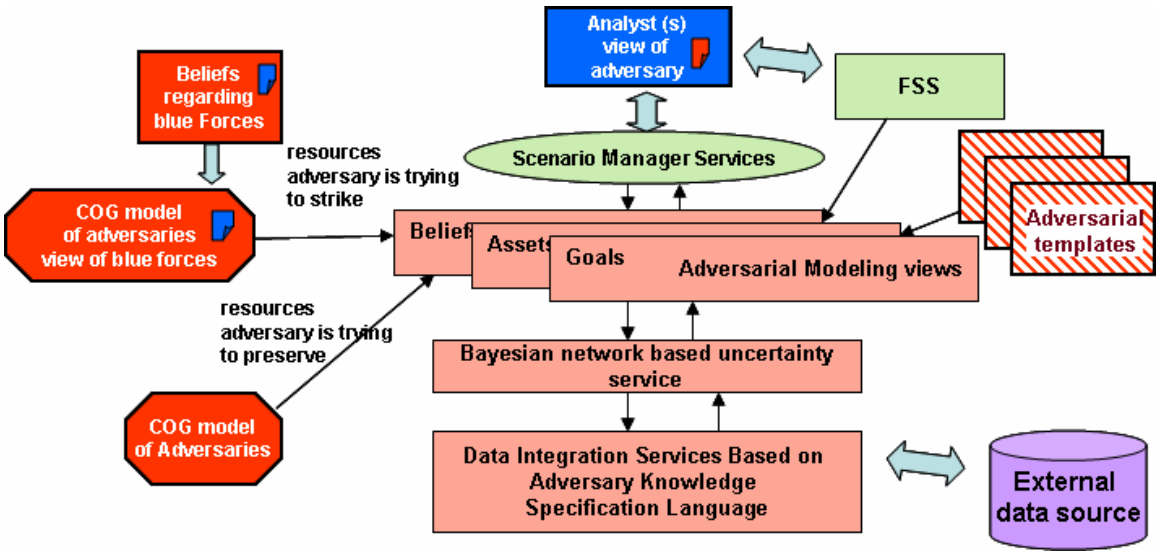


Figure 1 Proof of Concept Demonstration

A "proof of concept" demonstration was based upon a defined thread of adversarial activity. This thread was represented in the Force Structure Simulation (Gilmour et al. 2005) DENY FORCE Scenario. The fictional DENY FORCE Scenario is shown in Figure 2.

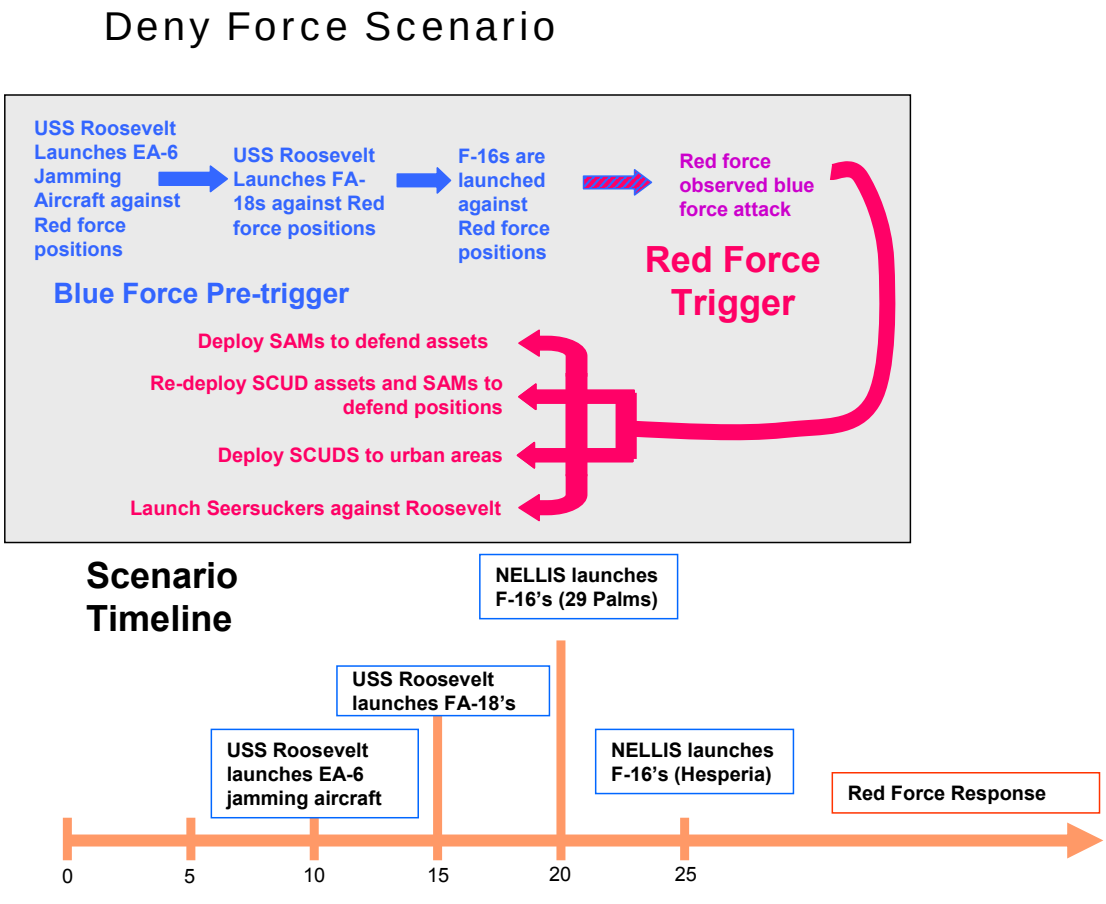


Figure 2 DENY FORCE Scenario

The EAMS POC defined all components necessary to support the demonstration. This included components developed as part of EAMS as well as existing systems. The EAMS POC Architecture along with applicable interfaces is shown in Figure 3. The EAMS components shown in Figure 3 are as follows:

1. EAMS Ontology (EO) – A web ontology language (OWL) used to describe data and semantic relationships between information necessary to support simulation of adversarial behavior.
2. Adversarial Intent Engine (AIE) – The AIE will generate alternative adversarial intent with probability assessments of those corresponding courses of action.
3. Adversarial Knowledge Specification Language (AKSL) – The AKSL is used to define adversaries and their capabilities from a series of lower level descriptions and general constraints. Will offer descriptions of adversarial data and semantic relationships.
4. AKSL Processor (AKSLP) – Will process AKSL to establish adversarial specifications within a specific instance of the EAMS ontology.
5. Intelligence/Situation Processor (ISP) – Will convert situational information for incorporation into the EAMS Ontology instance. The ISP populates observations of battlefield situation from a Red force perspective (i.e. observations by the Red force of operations being conducted by the Blue force). Can be used to provide real (observed) and hypothetical ("what-if") observations from multiple data sources. ISP will support the creation of "pop-up" adversaries or adversaries that appear suddenly in a battle scenario.
6. Scenario Manager Interface (SMI) – Component that will support a two-way interface between EAMS and the SGen Scenario Manager (Koziarz, Krause, Lehman, 2003). EAMS will communicate with simulation tools via the SGen Scenario Manager.
7. Adversary Action Engine (AAE) – Component will form the basic adversarial constructs from observables and serve as the primary interface to the AIE. Will extract the EO instance of the current adversary and develop Red force or adversary COAs.
8. Visualization Engine (VE) – Component provides interface capabilities for analysts to view various result sets. Will employ elements of hyperbolic view capabilities employed by Securboration on the UPSYS program (McQueary et al, 2004).

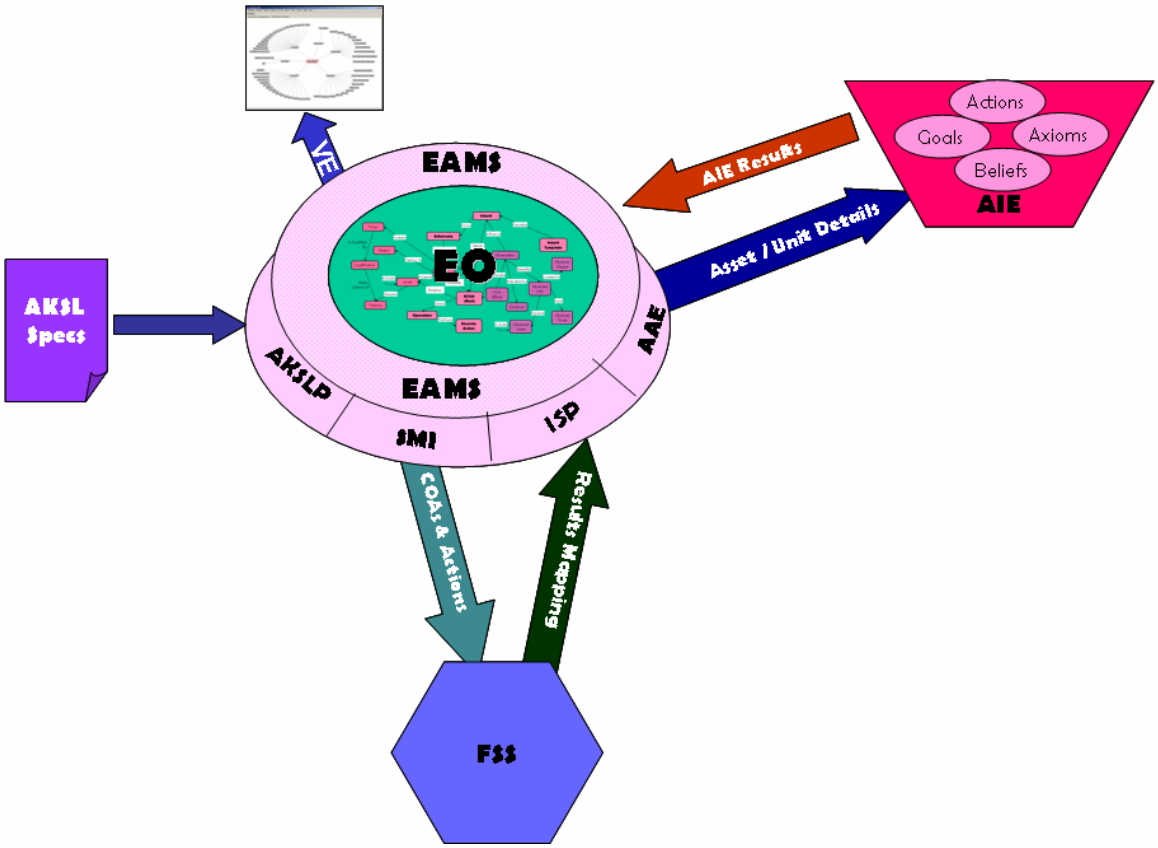


Figure 3 EAMS POC Architecture

The POC focused on demonstrating the ability to simulate emergent behavior of an adversary in a simulation environment and is based on the DENY FORCE Scenario as documented by AFRL and implemented within the Force Structure Simulation (FSS). The POC configured the DENY FORCE FSS simulation with a set of defined Blue missions that utilize Blue assets to attack and destroy Red assets.

The scenario consists of three main thrusts by the Blue force:

1) Launch EA-6's from USS Roosevelt to jam Red force radar at:
   - Meadows, Pendleton and Twentynine Palms
2) Launch FA-18's from USS Roosevelt at Red force positions:
   - Meadows and Pendleton
3) Launch F-16's from Nellis AFB at Red force positions:
   - Twentynine Palms and Hesperia

To fully demonstrate emergent behavior, no Red missions were defined a priori; instead, the EAMS POC relied on the AIE to generate candidate commander actions that would become the executed Red missions. To accomplish this, the EO was configured with:

1) A set of actions that was possible for Red to perform,
2) A set of Red beliefs,
3) A set of Red axioms,
4) A set of goals.

Two scenarios were developed and simulated during the POC to highlight the notion that – given the execution of a set of Blue missions – it is possible that two Red commanders, differing only by their "intent", will perform a different set of actions in response to the same set of Blue missions. For the POC, one commander was defined as being "aggressive" while the second commander was defined as being "passive". The aggressive commander is likely to retaliate in response to Blue thrusts and the passive commander is likely to merely defend. The Blue events that trigger the Red commander's actions are listed below. Scenario 1 represents the aggressive commander; scenario 2 represents the passive commander.

Scenario 1

Commander Intent - Aggressive

Defend Initial Attack

Move SAM's into Meadows from Pendleton

React To Destruction

Launch Seersucker at USS Roosevelt from Vandenberg

Continue To Defend

Move SAM's into Twentynine Palms from Pendleton

Scenario 2

Commander Intent - Passive

Defend Initial Attack

Move SAM's into Meadows from Pendleton

Continue To Defend

Move SAM's into Twentynine Palms from Pendleton

Defend With Authority

Operate All SAMs's

Each of the functional components described in the EAMS architecture was implemented as a part of the proof of concept development. The significant events that were chosen for the POC are:

1) Meadows Detects FA-18's
2) Meadows Experiences Destruction
3) Twentynine Palms Detects F-16's
4) Upon the occurrence of a "significant event", the AIE is triggered by the AAE to generate the list of potential Red actions that correspond to the event.

Once the candidate actions are generated by the AIE, EAMS generates the specific instance of a mission. The mission instance is driven by the implementation used by FSS to execute the mission.

The EAMS proof of concept successfully demonstrated the feasibility of using adversarial intent to influence adversarial response. As the application becomes more robust, we expect to demonstrate expanded capabilities, including the expansion of adversary parameterization and its effect on the rapid assembly and evaluation of adversarial response. Intent based adversarial response simulations will enable military planners and analysts additional tools in the assessment of battlefield scenarios.

Conclusion

The focus of the EAMS research project was to demonstrate that a realistic model of adversarial response could be created which is driven by the overarching intent of adversaries. Typical adversary response solutions supported limited adversary actions often based upon doctrine warfare approaches with limited or no dynamic response. EAMS set out to demonstrate that a realistic model of adversarial response could be constructed that would permit military planners and analysts increased fidelity in evaluation of battle plans against a less predictable adversary.

The critical elements of EAMS were systematically and comprehensively addressed. The approach yielded evidence that the Securboration team's approach can improve adversarial reasoning and simulation capabilities for:

- Modeling and prediction of adversary intentions and the direct and indirect relationships to adversary beliefs, perceptions, goals, and actions
- Capability for explaining adversary goals, intentions, and actions readily facilitates what-if analyses

Adaptation over time and predictions under uncertainty of the adversary provides the concept of evolving long-term and short-term goals and intentions, founded upon probabilistic uncertainty.

A robust and dynamic solution is achieved by providing a rich, interactive framework that centers on real-time continuous feedback between system components. EAMS

actively collaborates with the analyst, to assist in mission planning, addressing adversarial actions and reactions.

Adversary intent prediction cognitive architectures (Santos 2003; Santos and Negri 2004) that are part of the Securboration team's core technologies have been effectively and efficiently deployed in military planning and wargaming systems within the Air Force Research Laboratories' Force Structure Simulation Program (Surman, Hillman, and Santos 2003) and Lockheed Martin's Advanced Technology Laboratory projects in information fusion and distributed computing. Adversarial modeling and Scenario Generation efforts also served as a key technology in the Air Force's Effects-Based Operations program.

The initial research and development of EAMS demonstrated several key concepts:

- Intent can be used effectively to influence the actions of an adversarial force. Soft factors, such as the aggressive stance of an adversary force commander, can alter adversary response.
- EAMS can interact with existing Blue force simulations and create a realistic adversarial response to enable a fluid, more realistic battlefield simulation.
- The EAMS component architecture can interface with existing systems and technologies, including simulation applications currently in use in the Air Force.
- Descriptive elements of adversary composition can be parameterized, allowing for the rapid assembly and modification of an adversary force.
- Through the use of EAMS technology, a battlefield simulation can realistically represent the "push – pull" that exists in real-world battlefield scenarios.

As research continues in subsequent phases of EAMS, the foundations described here will be further refined and expanded.

Future Plans for EAMS Development and Deployment

Future development plans for EAMS will expand upon the capabilities explored during initial development. Plans call for EAMS to be incorporated in additional simulation environments and expansion into other areas, including effects based assessment and intelligence fusion applications, which call for adversary response prediction. Specific elements of EAMS to be expanded include the adversary parameterization and the application of Bayesian knowledge bases to represent uncertainty. Additional focus will be directed towards support of "what-if" analysis.

As part of the next phase of EAMS development, a full-scope prototype will be constructed. Its technology and architecture will be an expansion of the proof of concept built to demonstrate the EAMS approach.

As EAMS capabilities are expanded the Securboration team expects to construct a system capable of full support of realistic adversary response simulations based on varying levels of adversary intent.

Acknowledgements

The research described in this paper was funded under a Small Business Innovative Research (SBIR) contract from the Air Force Research Laboratory in Rome, NY. The Phase I award, entitled Campaign Level Adversarial Modeling System (Contract Number FA8750-04-C-0118) was completed in January of 2005. At the time of this writing, a Phase II award for continued research is pending.

References

Santos E. Jr., A Cognitive Architecture for Adversary Intent Inferencing: Knowledge Structure and Computation, Proceedings of the SPIE 17th Annual International Symposium on Aerospace/Defense Sensing and Controls: AeroSense 2003, Orlando, FL, 2003.

Santos E. Jr. and Negri A., Constructing Adversarial Models for Threat Intent Prediction and Inferencing,Proceedings of the SPIE Defense & Security Symposium, Vol. 5423, Orlando, FL 2004.

Fayette D.F, 2001, Effects-Based Operations: Application of New Concepts, Tactics, and Software Tools Support the Air Force Vision for Effects-Based Operations, AFRL Technology Horizons, Available at:
http://www.afrlhorizons.com/Briefs/June01/IF00015.html.

Surman J., Hillman R. and Santos E. Jr., 2003, Adversarial Inferencing for Generating Dynamic Adversary Behavior, Proceedings of the SPIE 17th Annual International Symposium on Aerospace/Defense Sensing and Controls: AeroSense 2003, Orlando, FL. 2003.

Grabo C.M., 2002, Anticipating Surprise: Analysis for Strategic Warning. (ed) Goldman J., Center for Strategic Intelligence Research, Joint Military Intelligence College.

Gilmour D., Hanna J., Koziarz W., McKeever W. and Walter M., 2005, High-Performance Computing for Command and Control Real-Time Decision Support, AFRL Technology Horizons, Available at:
http://www.afrlhorizons.com/Briefs/Feb05/IF0407.html.

Koziarz, Walter A., Krause, Lee S., Lehman, Lynn A., "Automated Scenario Generation," SPIE 17th Annual International Symposium on AeroSense Enabling Technologies for Simulation Science, Cambridge, MA, April 21-25, 2003

McQueary B., Krause. L., Santos E. Jr., Wang H., and Zhao Q., 2004, Modeling, Analysis and Visualization of Uncertainty in the Battlespace, 16th IEEE International Conference on Tools with Artificial Intelligence (ICTAI 2004).

Whittaker G.M., 2000, Asymmetric Wargaming: Toward A Game Theoretic Perspective.

Intent Driven Adversarial Modeling

June 14, 2005

Lynn Lehman
llehman@securboration.com

Duane A. Gilmour
duane.gilmour@rl.af.mil

Lee Krause
lkrause@securboration.com

Dr. Eugene Santos
eugene@cse.uconn.edu

Dr. Qunhua Zhao
qzhao@engr.uconn.edu

Agenda

- Adversary Modeling
- Increased Demands on the Planning Paradigm
- Emergent Adversarial Modeling
- The EAMS Intent Driven Approach
- EAMS “Proof of Concept” Demonstration
- EAMS Expansion
- Acknowledgements

Adversary Modeling

- **The increase in limited conflict warfare has created new challenges in mission planning and simulation.**
- **New approaches to warfare planning, such as effects based operations and predictive battlespace awareness, have also increased the need for improved simulations.**
- **Current adversarial simulation requires continual assessment of friendly courses of action and is currently "human assessment capability" limited.**
- **In the post-cold war era of limited conflict and unconventional adversary response, simulations based on attrition principles do not yield realistic or useable results.**
- **Modern elements of military intelligence and decision making require predictions of adversary force actions and reactions to provide a complete and realistic viewpoint.**

Increased Demands on the Planning Paradigm

- **Traditionally, Blue COAs are wargamed against the "most likely / dangerous" adversary COAs** *(as a pre-scripted sequence of events independent of Blue actions)*
- **Important to create and exercise realistic adversary responses as part of simulation for mission planning**
- **Non-conventional adversaries seldom have capabilities that rival U.S. forces adversarial intent and response become more important**
- **In the post-cold war era of limited conflict and unconventional adversary response, attrition- based simulations do not yield realistic results.**
- **Assessment / re-assessment of friendly courses of action is currently limited by human capability**
- **Need to model dynamic adversary behaviors that integrate with various intelligence and mission data sources (Modernized Integrated Database (MIDB), Air Operations Database (AODB), IPB Products, etc.**
- **The Emergent Adversarial Modeling System (EAMS) addresses operational patterns, behaviors, and doctrines of present-day adversaries (terrorist cells, local insurgents, guerillas, and armed thugs) as well as more conventional force elements.**

Emergent Adversarial Behavior

What is the concept of Emergent Adversarial Behavior

- **Emergent behavior refers to intelligent dynamic adversarial actions generated at the operational level in response to the execution of the friendly force within the simulation**
- **Red Force reacts to Blue Force actions (from their perspective**
  - **Monitor and understand battle-space *observables* and how they relate to *adversary* intent**
  - **Form a mission or missions (*reacting*) based on the *observables***
- **Red Force intent drives their actions**
  - **Missions differ based on differing intent**
- **Predictive adversary modeling is one of the key requirements for EBO, where the adversary is addressed as a system.**

Emergent Adversarial Modeling

- **EAMS demonstrates alterations of Red force behavior in response to observed Blue force actions.**
- **Blue force actions are addressed from the perspective of the Red force (i.e. what does Red think or believe that Blue is doing)**
- **The adversary force reacts, and also learns from and adapts to Blue force actions**
- **Adversarial behavior emerges during the interactions/encounters between Red force and Blue force**
- **Plans and strategies, which result in courses of action (COAs), are evaluated to determine the necessary steps to meet the overall strategic objectives.**
- **COA analysis, also defined as wargaming, is the process of performing "what if" analysis of actions and reactions designed to visualize the flow of the battle and evaluate each friendly COA**
- **The uncertainty of the adversarial decision process makes it necessary to evaluate friendly COAs against a range of adversary COAs.**

The EAMS Intent Driven Approach

- **Soft factors are those factors that influence adversarial intent in their decision making process, which include social, cultural, religious, political, economic and psychological issues.**
- **A significant amount of uncertainty is associated with any emergent adversarial actions**
- **Goals/Foci**: A prioritized (by probability) list of short and long term goals representing adversary intents, objectives or foci. The goal component captures ***what*** the adversary is doing.
- **Rationale Network**: A probabilistic network representing the influences of the adversary's beliefs, both about themselves and their opposition, on their goals and on high level actions associated with those goals. The rationale component infers ***why*** the adversary is behaving in a certain fashion.
- **Actions Network**: A probabilistic network representing the detailed relationships between adversary goals and possible actions to realize those goals. The action component captures ***how*** an adversary might act.

The EAMS Intent Driven Approach

- **Adversary axioms (X)** – represent the underlying beliefs of the adversary about themselves (vs. beliefs about Blue forces). Axioms typically serve as inputs or explanations to the other RVs, such as adversary goals.
- **Adversary beliefs (B)** – represent the adversary's beliefs regarding Blue forces (e.g., an adversary may believe that U.S. forces will not destroy religious sites or shrines).
- **Adversary goals (G)** – represent the goals or desired end-states of the adversary (e.g., preserving launchers, damage world opinion of U.S. action, defeat U.S. foreign policy, etc.).
- **Adversary actions (A)** – represent the actions of the adversary that can typically be observed by Blue forces.

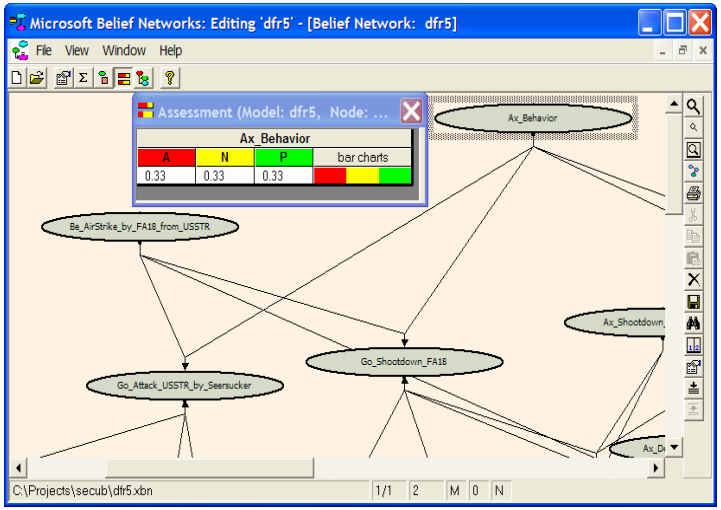
The EAMS Intent Driven Approach

- **EAMS takes inputs from multiple sources:**
  - **Evidence/observables from battlefield, recon, sensor arrays, etc.**
  - **Projected Red COAs from the adversarial specification represented by an instance in the EAMS Ontology.**
  - **Analyst inputs from the Intelligence Situation Processor (ISP) component of EAMS, critical to merging and working with human analysts.**

Behavior and Affects

Ax_Behavior represents a soft factor of red (commander).

Three states:
Aggressive,
Neutral,
Passive



Assessment (Model: dfr5, Node: Go_Shootdown_FA18)

Parent Node(s)			Go_Shootdown_FA18		
Ax_ShootDown_FA18	Be_AirStrike_by_FA18_from_USSTR	Ax_Behavior	Yes	No	bar charts
Yes	Yes	A	0.766	0.234	
		N	0.649	0.351	
		P	0.433	0.567	
	No	A	0.649	0.351	
		N	0.474	0.526	
		P	0.316	0.684	
No	Yes	A	0.474	0.526	
		N	0.211	0.789	
		P	0.141	0.859	
	No	A	0.374	0.626	
		N	0.061	0.939	
		P	0.041	0.959	

Assume the probability for the neutral states (N) is p_n,
The Probability for aggressive states (A) is: p_n + 0.33 * (1.0 - p_n)
The Probability for passive states (P) is: (1- 0.33) * p_n

Generate BKFs based on Ontology/KB

- **Generate the Beliefs**
  - **Beliefs: what red believes that blue is going to do**
  - **Identify possible pairs of blue units/assets attacking red units/assets**
  - **Generate a Belief for each pair**
    - **Search through previous cases**
    - **Identify new Beliefs where the pair is not covered previously and match to closest historical frequency data**
- **Generate the Axioms**
  - **Axioms: what red believes about themselves**
  - **Identify red units/assets**
  - **Generate axioms for:**
    - **Status: for example, the operation condition of a airport**
    - **Effectiveness: Probability of hitting of the target with the asset, etc.**

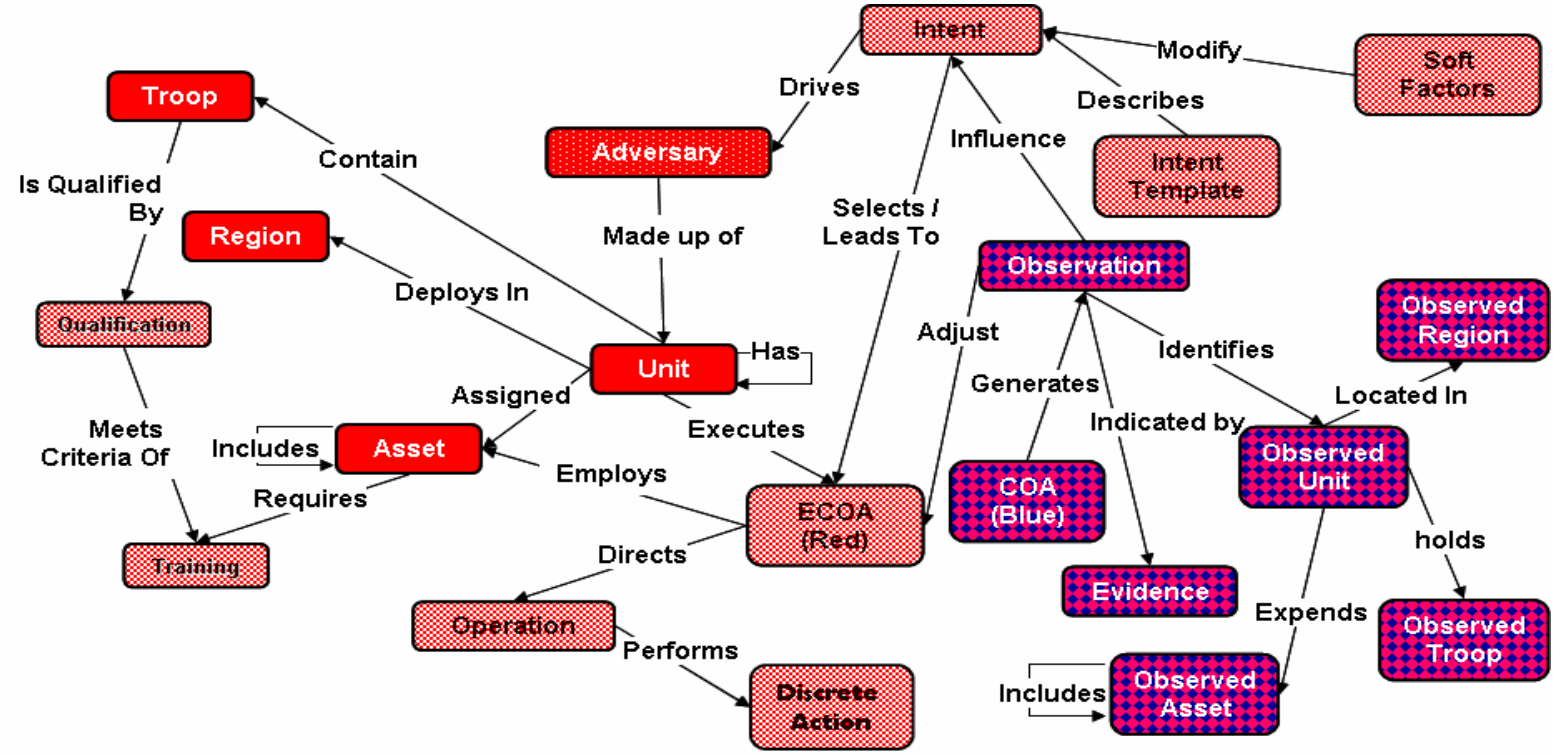
Generate BKFs (cont..)

- Generate the Beliefs and Axioms Based on
  - What are the doctrines defined in the ontology
  - What red/blue has: units/assets
  - What red believes the units/assets can do
  - Frequency data from history (database)
  - Examples:
    - No surrender (Ax_Surrender, yes = 0.01, no = 0.99)
    - Has 12 seersuckers (Ax_Has_Seersucker_12)
    - Seersucker has a single-shot hit probability of 70%, but blue can block it with 85% chance (Ax_Hit_Target_by_Seersucker_1, yes = 0.105, no = 0.895)

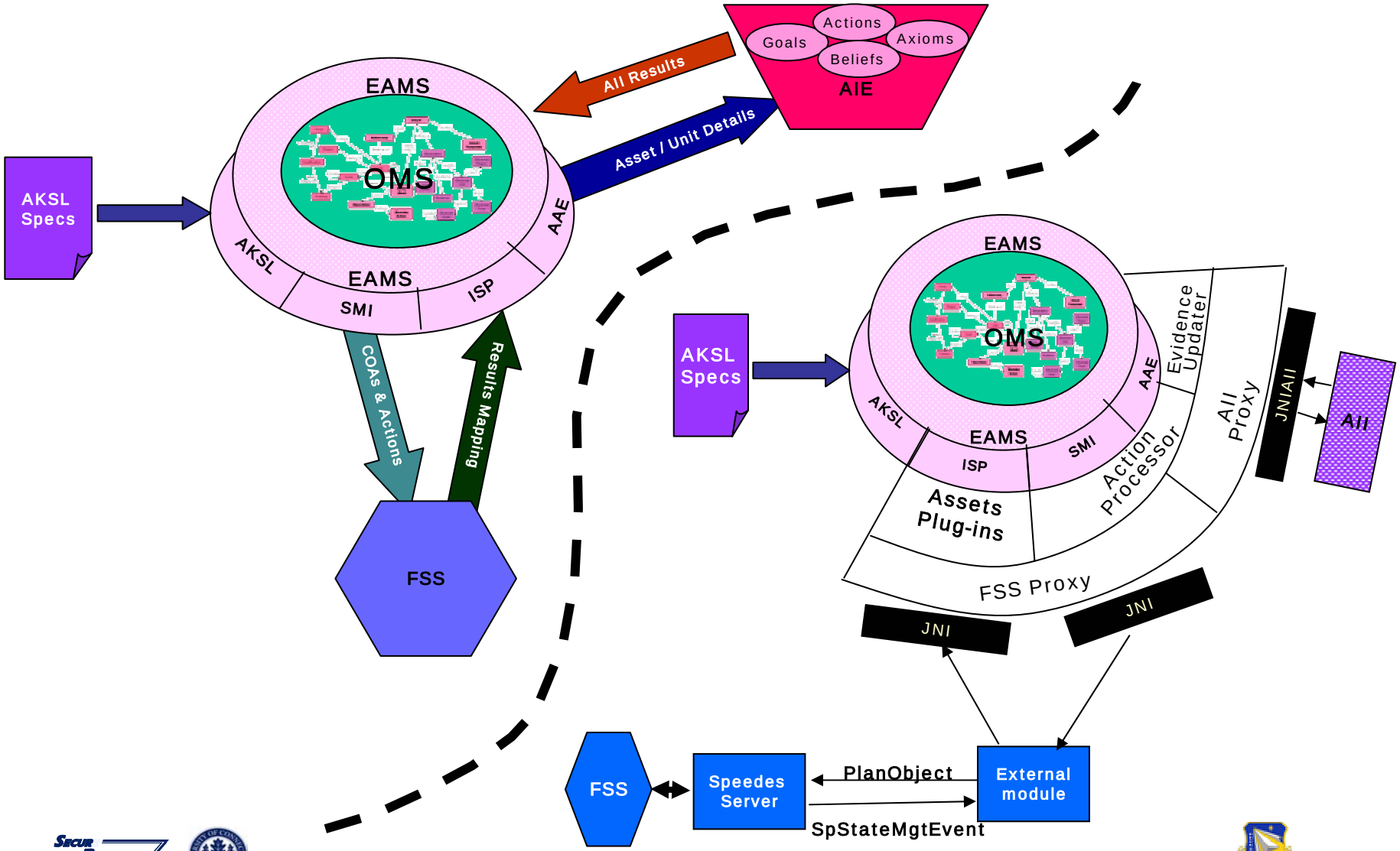
Proof of Concept Demo

- Demonstrated fluid (dynamic) adversarial response based upon observations of Blue Force actions
- Utilized Securboration's Scenario Generation Service (SGen) to support COA generation (Red and Blue Force COAs possible)
- Demonstrated (on limited basis) a structured adversary specification
- Deny Force Scenario running on the Force Structure Simulation
  - Demonstrated alternate Red Force responses
  - Supported actions driven by adversary's intent

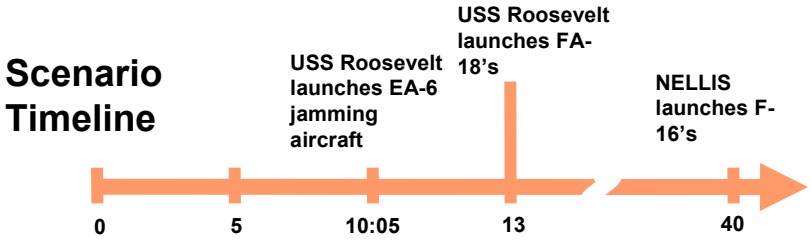
EAMS Ontology

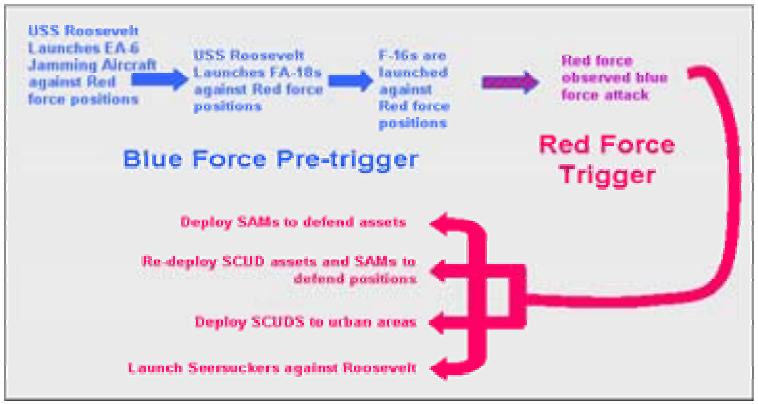


POC Architecture and Implementation



Deny Force Scenario





Demo Scenario 1

Significant Observable Events

- Meadows Detects Enemy
- Meadows Experiences Destruction
- Twenty Nine Palms Detects Enemy

Commander Intent - Aggressive

- Defend Initial Attack
  - Move GOA's into Meadows from Pendleton
- React To Destruction
  - Launch SeerSucker at USSTR from Vandenberg
- Continue To Defend
  - Move GOA's into Twenty Nine Palms from Pendleton

Demo Scenario 2

Significant Observable Events

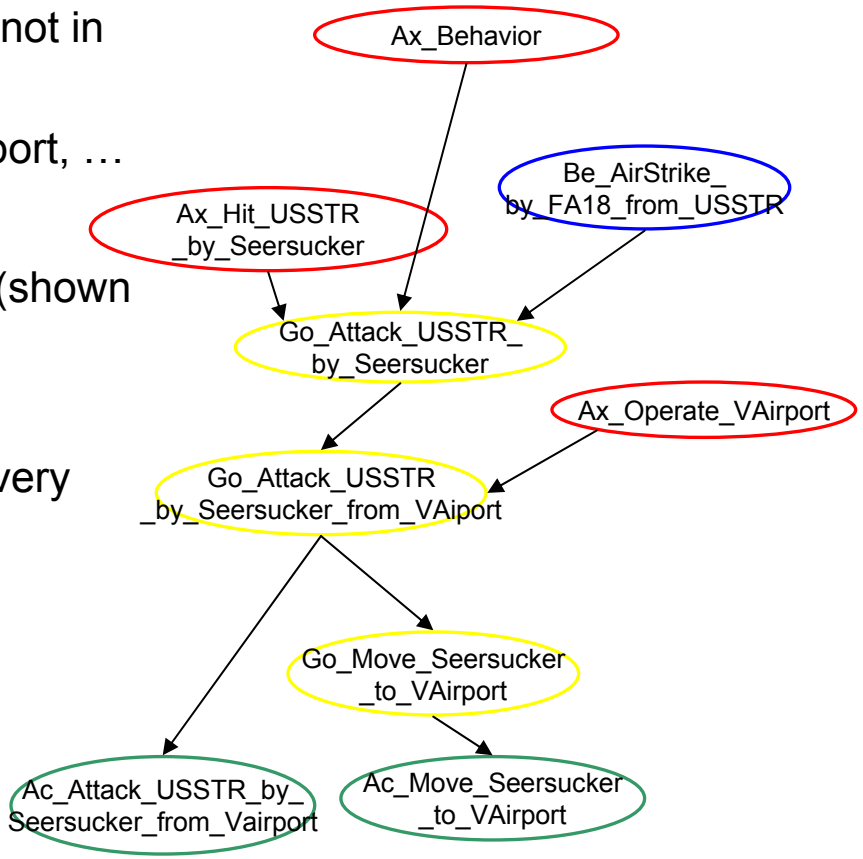
- Meadows Detects Enemy
- Meadows Experiences Destruction
- Twenty Nine Palms Detects Enemy

Commander Intent - Passive

- Defend Initial Attack
  - Move GOA's into Meadows from Pendleton
- Continue To Defend
  - Move GOA's into Twenty Nine Palms from Pendleton
- Defend With Authority
  - Operate All SA-2's

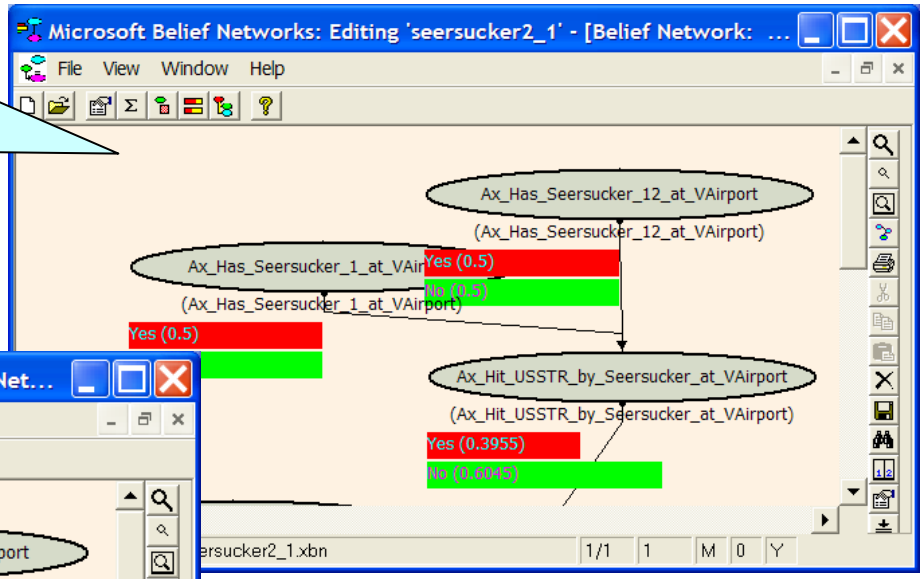
An example of BKF generation

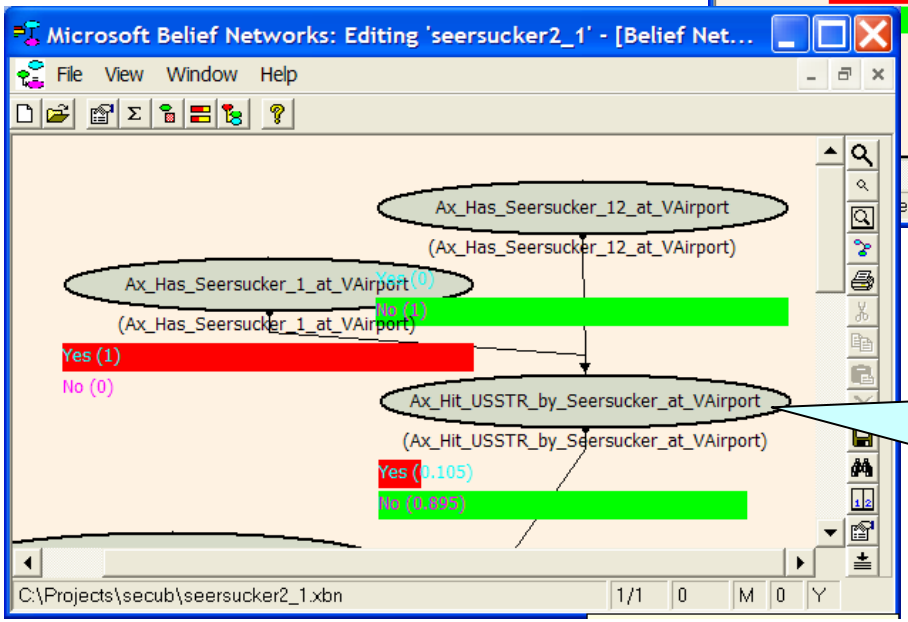
- According to the scenarios, there is a goal to attack USS TR with sunburn, which is a new asset not in the working network.
  - Assets include: USS TR, sunburn, VAirport, …
- Search in the library retrieves one fragment (shown next)
  - Include, USS TR, VAirport, seersucker.
  - Also the goals, axioms, and beliefs are very similar



Represent numbers of assets in BN

Red possibly has 1 or 12 seersuckers from 2 different reports. Hit
p(yes = 0.3955, no =0.6045)



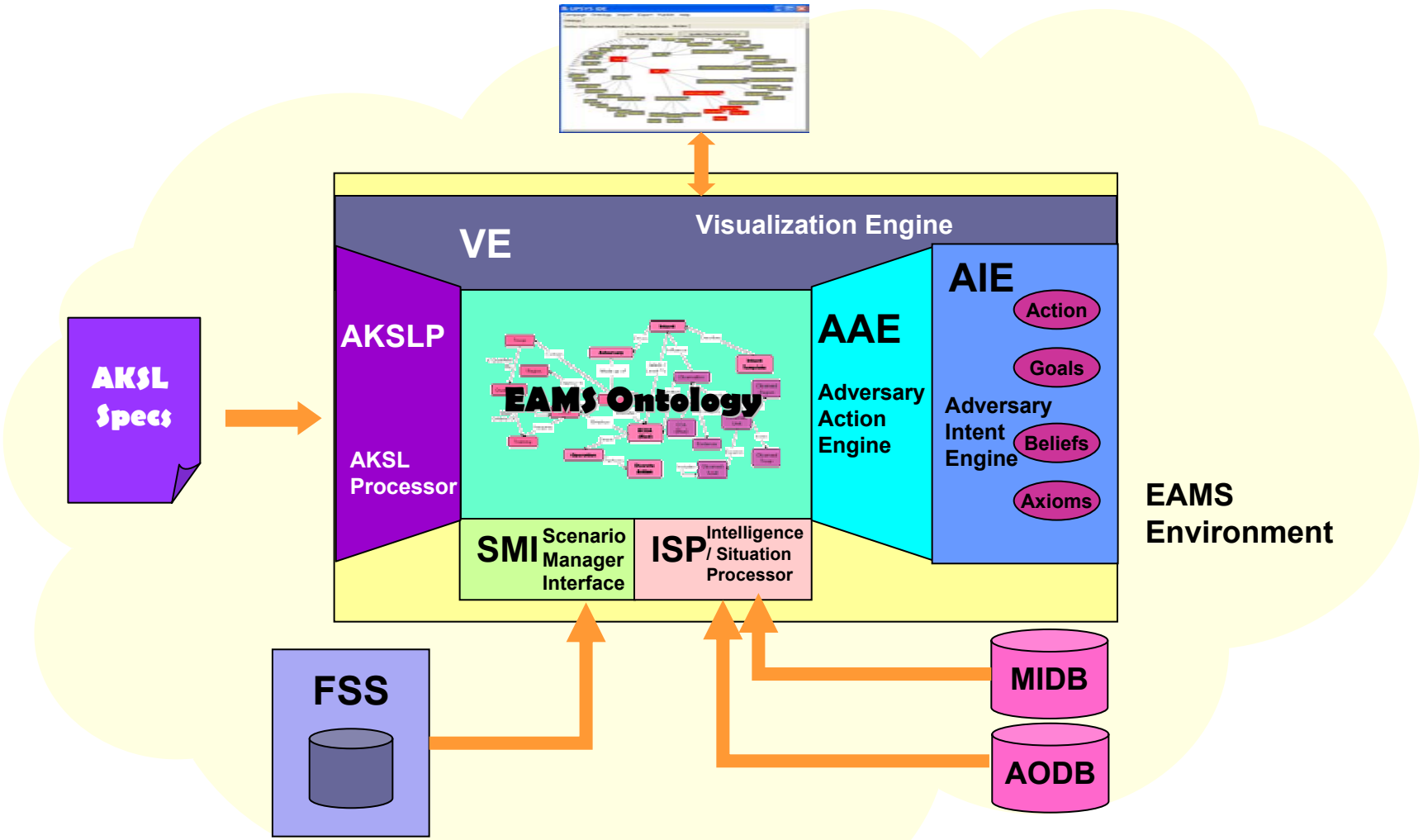


Now confirmed, they only have 1 seersucker.
Hit
p(yes = 0.105, no =0.895)

EAMS Phase I

- Completed a robust EAMS Ontology Framework
  - Provides Support for Adversary Parameterization
  - Supports “build-up” or enhancement of adversary capabilities
- Established EAMS Components Interaction Framework
- Completed Proof-of-Concept Demonstration
  - Emergent behavior (red forces action to blue force observables)
    - Ability to develop COA based on observables
  - Intent driven adversary
  - Observables that drive the scenario are captured in EAMS
  - Ability to recreate complete scenarios for future analysis

Prototype Architecture Phase II



Architecture Components

- **EAMS Ontology (EO)**
  - **OWL based ontology**
  - **Describes data and semantic relationships between information necessary to support simulation of adversarial behavior.**
- **Adversarial Intent Engine (AIE)**
  - **Formerly All**
  - **Will generate alternative adversarial intent with probability assessments of those corresponding courses of action.**
- **Adversarial Knowledge Specification Language (AKSL)**
  - **Used to define adversaries and their capabilities from a series of lower level descriptions and general constraints.**
  - **Will offer descriptions of adversarial data and semantic relationships.**

Architecture Components cont..

- **AKSL Processor (AKSLP)**
  - **Interpreter to process AKSL**
  - **Will establish adversarial specification within a specific ontology instance**
- **Intelligence / Situation Processor (ISP)**
  - **Will convert situational information for incorporation into the EAMS Ontology instance.**
  - **Bulk will populate observations of battlefield situation from a Red force perspective (i.e. Observations by the Red force of operations being conducted by the Blue force.)**
  - **Can be used to provide real (observed) and hypothetical ("what-if") observations from multiple data sources.**
  - **Will support creation of "pop-up" adversaries or adversaries that appear suddenly in a battle scenario.**

Architecture Components cont..

- **Scenario Manager Interface (SMI)**
  - **Will support a two-way interface between EAMS and the SGen Scenario Manager.**
  - **EAMS will communicate with simulation tools via the SGen Scenario Manager.**
- **Adversary Action Engine (AAE)**
  - **Component will form the basic adversarial constructs from observables and serve as the primary interface to the AIE.**
  - **Will extract the EO instance of the current adversary and develop Red Force or adversary COAs**
- **Visualization Engine (VE)**
  - **Component provides interface capabilities for analysts to view various result sets.**
  - **Will employ hyperbolic view capabilities from Securboration's UPSYS program.**

Key Concepts Validated in Phase I

- **Adversarial modeling with a system focus on Emergent behavior**
- **Selectable adversary intent**
- **Ability to maintain current status of observables in the SMI**
- **Demonstrated the relationships between observables, axioms, beliefs to support the generation of candidate actions and goals**
- **Logging of interaction to support play back analysis**
- **Algorithm/method for generating BKFs from Ontology/KB**
- **Base probabilities of red capabilities change as red units/assets change**
- **Systematic mechanism for parameterization / alteration of Red behavior based on soft factors**

Contact and Additional Info

For additional Information contact

Lee Krause

Securboration Inc

321.591.9836

lkrause@securboration.com

Acknowledgements

The research described in this paper was funded under a Small Business Innovative Research (SBIR) grant from the Air Force Research Laboratory in Rome, NY. The Phase I award, entitled Campaign Level Adversarial Modeling System (Contract Number FA8750-04-C-0118) was completed in January of 2005. The research is currently progressing under a Phase II grant.

- Santos E. Jr., A Cognitive Architecture for Adversary Intent Inferencing: Knowledge Structure and Computation, Proceedings of the SPIE 17th Annual International Symposium on Aerospace/Defense Sensing and Controls: AeroSense 2003, Orlando, FL, 2003.
- Santos E. Jr. and Negri A., Constructing Adversarial Models for Threat Intent Prediction and Inferencing,Proceedings of the SPIE Defense & Security Symposium, Vol. 5423, Orlando, FL 2004.
- Fayette D.F, 2001, Effects-Based Operations: Application of New Concepts, Tactics, and Software Tools Support the Air Force Vision for Effects-Based Operations, AFRL Technology Horizons, Available at:
- http://www.afrlhorizons.com/Briefs/June01/IF00015.html.
- Surman J., Hillman R. and Santos E. Jr., 2003, Adversarial Inferencing for Generating Dynamic Adversary Behavior, Proceedings of the SPIE 17th Annual International Symposium on Aerospace/Defense Sensing and Controls: AeroSense 2003, Orlando, FL. 2003.
- Grabo C.M., 2002, Anticipating Surprise: Analysis for Strategic Warning. (ed) Goldman J., Center for Strategic Intelligence Research, Joint Military Intelligence College.
- Gilmour D., Hanna J., Koziarz W., McKeever W. and Walter M., 2005, High-Performance Computing for Command and Control Real-Time Decision Support, AFRL Technology Horizons, Available at:
- http://www.afrlhorizons.com/Briefs/Feb05/IF0407.html.
- Koziarz, Walter A., Krause, Lee S., Lehman, Lynn A., "Automated Scenario Generation," SPIE 17th Annual International Symposium on AeroSense Enabling Technologies for Simulation Science, Cambridge, MA, April 21-25, 2003
- McQueary B., Krause. L., Santos E. Jr., Wang H., and Zhao Q., 2004, Modeling, Analysis and Visualization of Uncertainty in the Battlespace, 16th IEEE International Conference on Tools with Artificial Intelligence (ICTAI 2004).
- Whittaker G.M., 2000, Asymmetric Wargaming: Toward A Game Theoretic Perspective.